Implanted atoms create unique electrical IDs that distinguish bona fide devices from forgeries

September 16 2021

Credit: CC0 Public Domain

If someone sells you a luxury handbag from Paris, France, but it turns out be a forgery from Paris, Texas, the counterfeit item might cost you a

thousand bucks and the crook could wind up in jail. But if a counterfeit electronic device gets installed in a car, it could cost passengers or the driver their lives.

Without new security measures, the interconnected wireless technologies, digital electronics and micromechanical electronic systems that make up the Internet of Things are vulnerable to forgeries and tampering that could cause entire telecommunication networks to fail. In 2017, sales of counterfeit products of all sorts—from electronics to pharmaceuticals—amounted to an estimated $1.2 trillion worldwide.

To help prevent counterfeit computer chips and other electronic devices from flooding the market, researchers at the National Institute of Standards and Technology (NIST) have demonstrated a method that could electronically authenticate products before they leave the factory.

The scientists employed a well-known technique called doping, in which small clusters of "foreign" atoms of a different element from those in the device to be labeled are implanted just beneath the surface. The implanted atoms alter the electrical properties of the topmost layer without harming it, creating a unique label that can be read by an electronic scanner.

Using doping to create electronic tags for devices is not a new idea. However, the NIST technique, which uses the sharp tip of an atomic force microscope (AFM) probe to implant atoms, is simpler, less costly and requires less equipment than other doping techniques using lasers or a beam of ions, said NIST researcher Yaw Obeng. It is also less damaging than other methods.

"We're putting a sticker on every device, except that the sticker is electronic and no two are identical because in each case the amount and pattern of the dopant atoms is different," said Obeng.

To create the electronic ID, Obeng and his colleagues first deposited a 10-nanometer (billionth of a meter) film of dopant material—in this case aluminum atoms—about 10-centimeter-square silicon wafers that were then broken into postage-stamp-size fragments so that they could fit in the AFM. The team then used the needle-like tip of the AFM probe to push aluminum atoms a few nanometers into the silicon fragments. The diameter of the implanted regions was tiny, no larger than 200 nm.

The implanted atoms alter the arrangement of silicon atoms just beneath the surface of the wafer. These silicon atoms, as well as those that reside throughout the wafer, are arranged in a repeating geometric pattern known as a lattice. Each silicon lattice acts like an electrical circuit with a certain impedance, the AC (alternating current) equivalent of resistance in a DC (direct current) circuit.

When the implanted aluminum atoms were rapidly heated to about 600 degrees Celsius, a few of them acquired enough energy to replace some of the silicon in lattices just beneath the wafer's surface. The random substitution altered the impedance of those lattices.

Each dopant-modified lattice has a unique impedance depending on the amount and type of dopant. As a result, the lattice can serve as a distinctive electronic label—a nanometer-scale version of a QR code for the wafer, Obeng said. When a scanner directs a beam of radio waves at the device, the electrically altered lattices respond by emitting a unique radio frequency corresponding to their impedance. Counterfeit devices could be easily identified because they would not respond to the scanner in the same way.

"This research is key because it offers a means to uniquely identify components by a secure, unalterable and inexpensive means," said Jon Boyens, a researcher with NIST's Computer Security Division who was not a co-author of the study.

The study, which Obeng presented on Sept. 16 at the International Conference on IC Design and Technology in Dresden, Germany, builds upon earlier work by the same team . The new study refines the AFM method for inserting dopant atoms, so that the AFM probe can more precisely place the atoms in the silicon wafer. The higher precision will make it easier to test the electronic ID system under real-life conditions.

Obeng and his collaborators, who include Joseph Kopanski of NIST and Jung-Joon Ahn of NIST and George Washington University in Washington, D.C., consider their technique a prototype that will need modification before it can be used in mass production.

One possibility is to use the sharp probes of several AFMs working side by side so that the dopant material could be implanted in many devices at once. Another strategy would employ high-pressure rollers to rapidly push dopant atoms coating a computer chip or other device a few nanometers into the device. A pattern stenciled onto the rollers would ensure that the dopant atoms were implanted according to a precise blueprint. Rollers are widely used to smooth paper, textiles and plastics.

Obeng presented the work on Sept. 16 at the International Conference on IC Design and Technology in Dresden, Germany.

More information: Jung-Joon Ahn et al, Probe assisted localized doping of aluminum into silicon substrates, *Journal of Applied Physics* (2019). DOI: 10.1063/1.5065385

Provided by National Institute of Standards and Technology

Citation: Implanted atoms create unique electrical IDs that distinguish bona fide devices from forgeries (2021, September 16) retrieved 3 May 2024 from

https://phys.org/news/2021-09-implanted-atoms-unique-electrical-ids.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.